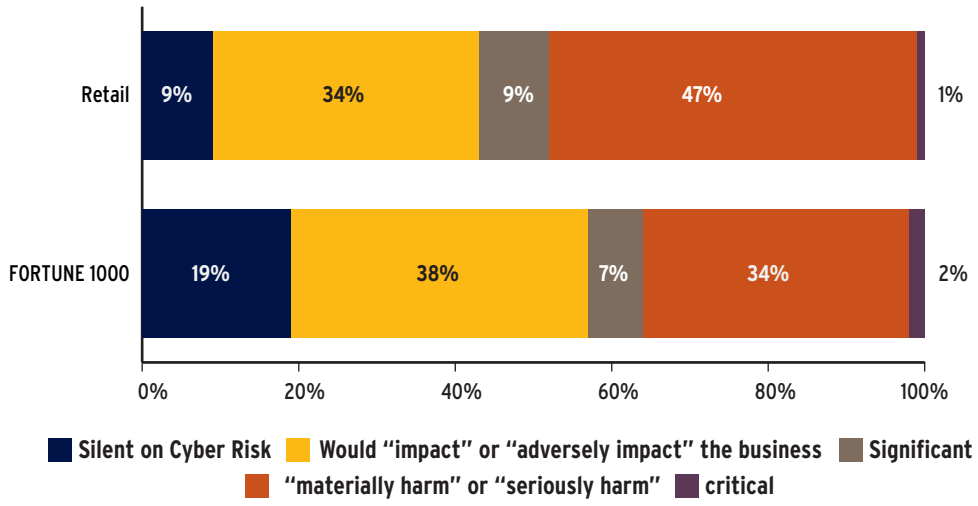
WILLIS SPECIAL REPORT: 10K DISCLOSURES – HOW RETAIL COMPANIES DESCRIBE THEIR CYBER LIABILITY EXPOSURES

This special report examines the cyber risk disclosures made by the retail sector of the Fortune 1000.[1] It is part of a Willis series reporting on how U.S. public companies are describing their cyber risks in financial documents as required by the guidelines published by the SEC in October 2011.

The retail industry has been the target of many of the most high profile system breaches which have resulted in some of the largest cyber losses. Willis found that the retail sector was much more likely than other Fortune 1000 sectors to disclose that cyber risk was significant, serious, material or critical (57%), and much less likely to be silent on the issue (9%) than the Fortune 1000 as a whole.

EXTENT OF CYBER RISK FORTUNE 1000 V RETAIL



"AT SOME POINT, THE CEO AND BOARD OF DIRECTORS HAVE TO ACCEPT RESPONSIBILITY..... IT HAS TO COME DOWN TO A POINT, A SOURCE POINT." SENATOR ROCKEFELLER IN A RECENT HEARING ON RETAIL BREACHES.

Willis

The latest Verizon Breach 2013 report[2], which reviews more than 47,000 breaches but focuses on analyzing 621 large breaches where there is enough data to verify details, shows that the retail sector has had the largest number of financial losses for 2012 in the large breach category. Further, the percentage of losses facing retailers that are financial in nature is higher than any other business category.

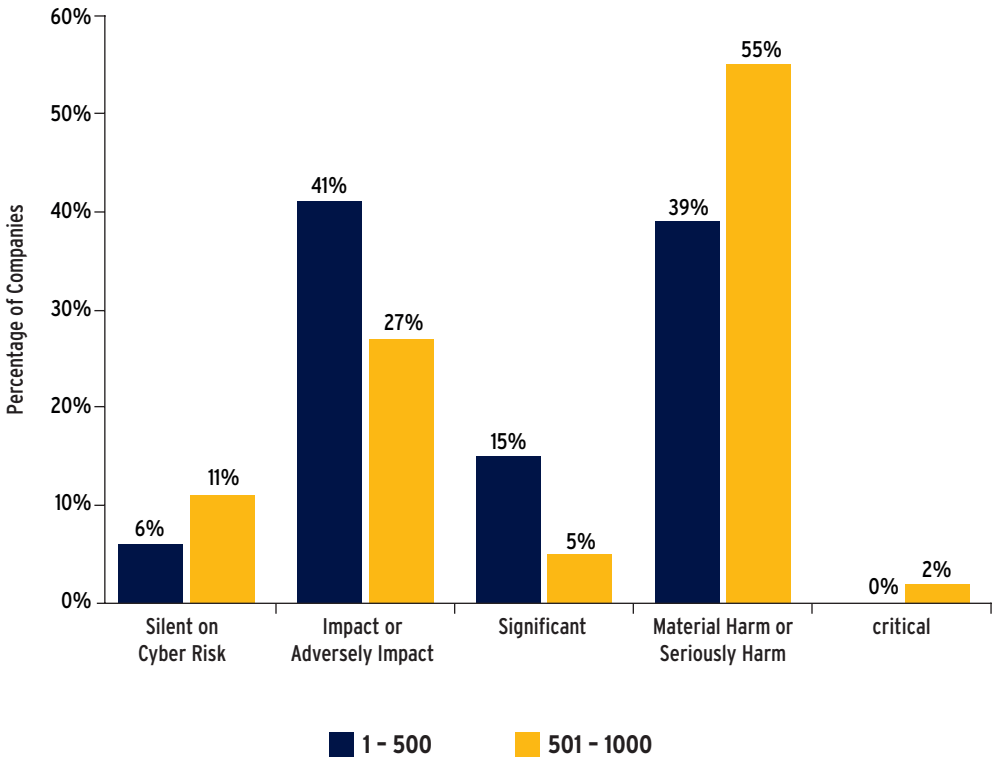
The Verizon survey shows retailers second, behind financial institutions, in the number of "impact" breaches (96 of the 621 breaches were retail companies).

EXTENT OF CYBER RISK

Although Willis found that the number of companies silent on cyber exposures was significantly smaller than for the Fortune 1000 as a whole, we were surprised, given the history of the segment for being the target of breaches, that any companies were silent on this issue. We found a gap between the Fortune 500 and the Fortune 501 – 1000. While 11% in the Fortune 501–1000 remained silent, only 6% of the Fortune 1000 were silent. However, more of the smaller Fortune 501–1000 companies deemed the risk serious, material or critical (57%) than some of their larger peers on the Fortune 1000 (39%).

We speculate that the smaller organizations believe they have fewer financial resources to withstand a significant attack than do the larger Fortune 500 companies, which may be more confident in their ability to marshal resources and withstand an event.

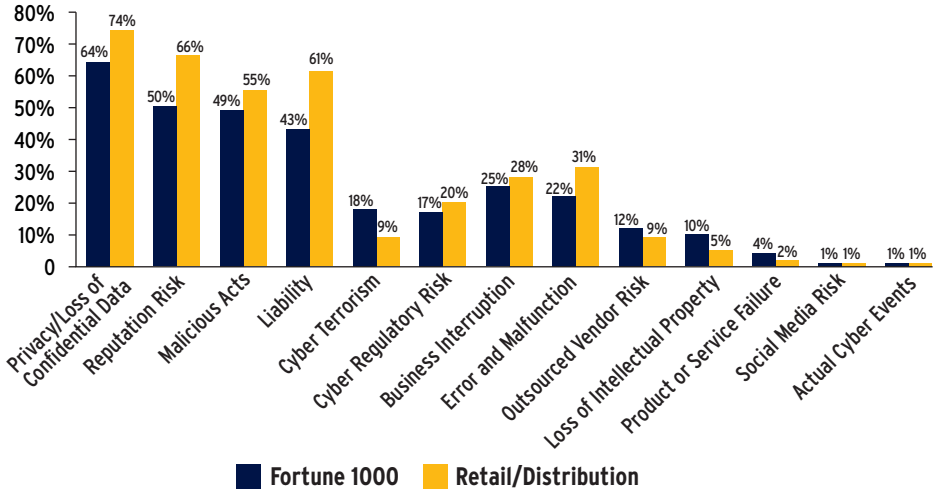
EXTENT OF CYBER RISK RETAIL FORTUNE 500 V F501 - 1000



KEY CYBER EXPOSURES FOR RETAILS

Willis found that the retail sector disclosed individual cyber risks at rates significantly higher than the Fortune 1000 as a whole. The most notable exposures disclosed at higher rates were: loss or disclosure of confidential information, loss of reputation, malicious acts and cyber liability.

REPORTED EXPOSURE F1000 V RETAIL/DISTRIBUTION



EVOLVING EXPOSURES: POINT OF SALE BREACHES

The end of 2013 saw a significant number of large credit card thefts at retailers involving breaches of point of sale devices. As a result, more than 100 civil actions have begun to cover the fraud and other costs. At a February 2014 Senate hearing on the issue, it was noted that United States holds 25% of the world's credit cards but suffers half the world's fraud.[3] It was also noted that there are seven times more fraud associated with debit card transactions that don't require a PIN than those that do.

This has prompted many to wonder why the rest of the world uses safer EMV3[4] ("chip-and-PIN") credit cards, but the United States still relies on less secure magnetic stripe technology. Chip-and-PIN cards that include a computer chip within the card and require a PIN to use were praised at the hearing for their ability to reduce fraud at the point of sale.

EMV3 technology is not a complete panacea. It would not have prevented many of the point-of sale breaches at retailers last year according to many IT security specialists.[5] If a breach occurs in the company's data center, EMV3 technology will not prevent the loss. The nature of the physical cards does not matter at that point. Card-not-present transactions will still also present fraud risks despite the introduction of chip-and-PIN technology.

Furthermore, although chip-and-PIN cards are more secure than magnetic stripe cards, most experts believe that the majority of cards in the U.S. will continue to have a magnetic stripe for many years to accommodate retailers who resist the MasterCard and Visa's demand to implement chip-and-PIN by 2015. Normally, the card issuer is liable for fraudulent transactions. However, if the ATM or merchant's point of sale terminal does not support EMV after certain dates, then the ATM owner or merchant will be liable for the fraudulent transaction. These liability shifts are due to take place starting April 2013 through 2017 depending on the type of card used.

EVOLVING EXPOSURES: MARKETING AND "DO NOT TRACK"

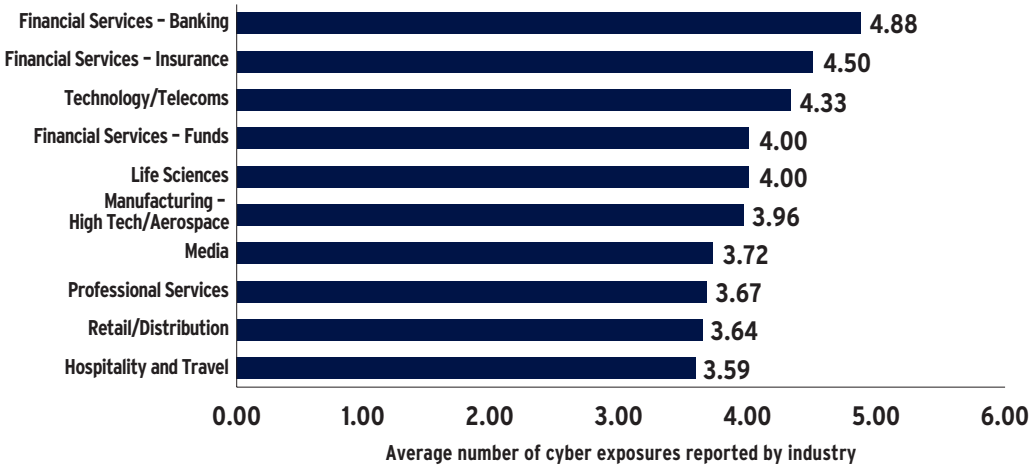
2013 became the year of the "do not track" class action. As of December 19, 2013, 183 "do not track" class actions were pending in the U.S., and the number is expected to grow. California has legislated stricter controls, effective January 1, 2014, under the California Online Privacy Protection Act.[6] While many of these actions are against social media and technology companies, a significant number name retailers as defendants.

Both the California Attorney General's office and the Federal Trade Commission have signaled that they will enforce both new and current consumer protection laws with diligence.[7] We expect other states to follow California's lead for stricter "do not track" legislation, as many of the 183 class action suits are outside of California.

FORTUNE 1000 – NUMBER OF CYBER EXPOSURES DISCLOSED BY INDUSTRY

When it comes to the number of cyber exposures disclosed, the retail sector is ninth on the list of industries, averaging 3.64 per company.

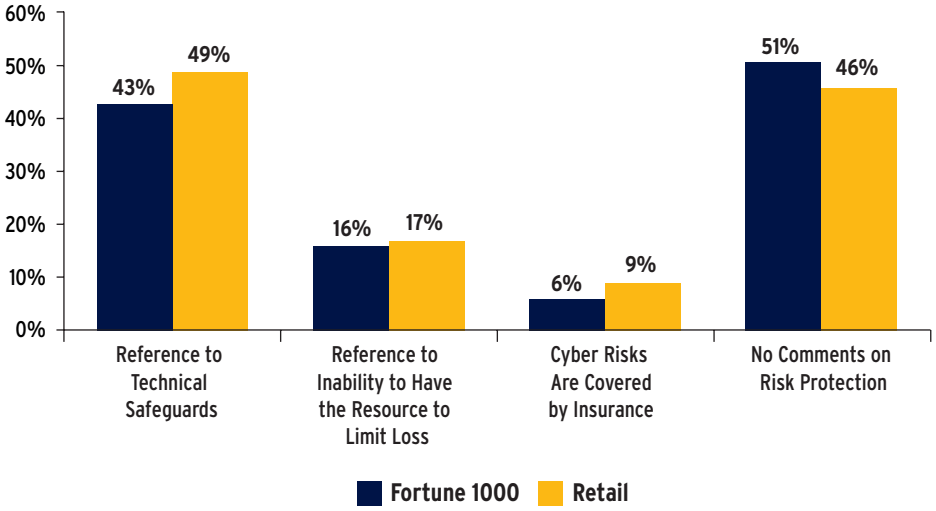
INDUSTRIES NOTING HIGHEST NUMBER OF CYBER RISK EXPOSURE IN FINANCIAL REPORTING DOCUMENT



CYBER RISK REMEDIES

To protect against cyber exposures, 49% of retail companies cited the use of technical safeguards – more than Fortune 1000 companies as a whole (43%). Our survey results indicated a potential cause for concern in that 17% of retail companies report inadequate resources to limit cyber losses, which usually indicates that technical protections may not be sufficient to contain the effects of some cyber or technology events.

REPORTED RISK MANAGEMENT FORTUNE 1000 V RETAIL

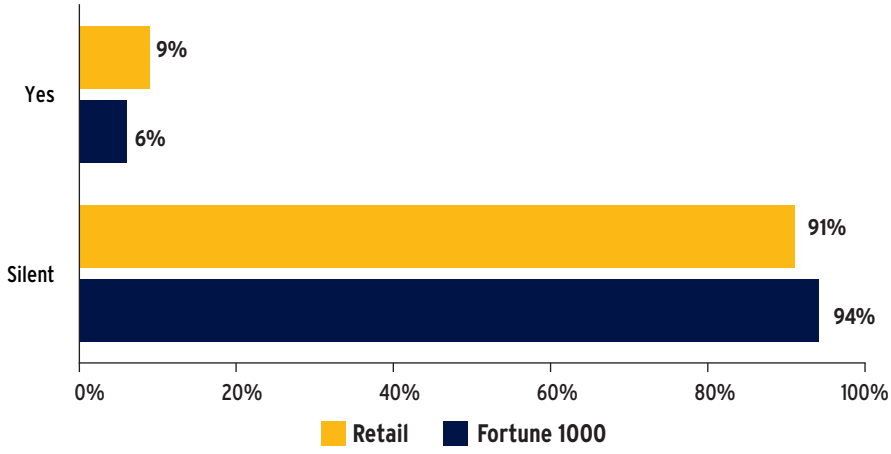


INSURANCE PROTECTION FOR CYBER EVENTS (NUMBER OF COMPANIES)

The retail sector ranks fourth in the Fortune 1000 when it comes to disclosing insurance as a protection against cyber events, with 9% indicating that they purchase insurance for their cyber exposures.

This places them below the funds sector (33%), utilities (15%), and banking and conglomerates (tied at 14% each), tech/telco and insurance (11%) and the media industry (10%).[8]

INSURANCE COVERAGE FORTUNE 1000 V RETAIL



SUSPECTED UNDERREPORTING OF INSURANCE

While public disclosure documents suggest that only 9% of retail companies buy cyber insurance, we believe that rate may be substantially higher. The take-up rate in other sectors that Willis has reviewed has been higher than the rate disclosed in the 10ks for those sectors.

Willis and cyber insurance underwriters recently conducted an informal survey of life and health insurance companies in the Fortune 1000. This survey found over 60% of these insurers purchased stand-alone cyber coverage. We conclude that many Fortune 1000 companies in the retail sector may be similarly under-reporting the purchase of insurance covering Cyber, Errors and Omissions Liability, or other insurance products that may provide protection against cyber events.

THE NATIONAL CYBERSECURITY FRAMEWORK

Due to the threats, risks and potential impact of cyber exposures to the nation's economy, security and critical infrastructure, President Obama issued the Executive Order, "Improving Critical Infrastructure Cybersecurity" on February 12, 2013. The Executive Order called for creating a voluntary, risk-based cybersecurity framework that is "prioritized, flexible, repeatable, performance-based, and cost-effective," and is to be developed and implemented in partnership with owners and operators of the nation's critical infrastructure.

The goal is to base the framework on practices developed, managed and updated ***by industry***, evolving with technological advances and aligning with business needs. It would establish a common structure for managing cybersecurity risk and help firms identify and understand their dependencies with business partners, vendors and suppliers.

The Department of Homeland Security is the U.S. government's lead agency for coordinating the protection, prevention, mitigation and recovery from cyber incidents. On February 12, 2014, the Obama administration released the "Framework for Improving Critical Infrastructure Cybersecurity" (the "NIST Framework").[9]

The NIST Framework is comprised of three primary components: the Framework Core, the Framework Implementation Tiers and the Framework Profiles. The Framework Core sets forth cybersecurity activities commonly employed across critical infrastructure sectors to achieve specific outcomes and provides examples of existing standards to facilitate implementation of those activities.

As companies in the retail sector begin to respond to the new framework, we may eventually see greater threat response leading to decreased cyber losses.

INTERDEPENDENCY AND RESILIENCY

A number of public and private groups have formed with the goal of addressing the evolving threats and risks that industries face; in particular, the 16 critical industries identified by DHS and the White House. The retail industry has not been identified as a critical industry and therefore has not been the target of an effort to have them share information between companies by government.

However, retail industry leaders say their sector now is considering several ways to better prepare for and defend against the increasing wave of targeted attacks on its members, including the formation of a Merchant and Retail Industry Information Sharing and Analysis Center (ISAC). The National Retail Federation (NRF) and other retail trade associations have teamed with key financial associations to explore more information-sharing, as well as the adoption of more secure payment cards.

THE FUTURE

Because of where retail companies sit in the economy with valuable credit card information and desirable goods, they have been prime targets of cyber criminals, hackers and disgruntled employees. As networks become more sophisticated and the degree of technology required by consumers grows, we expect the level of cyber exposures to expand accordingly.

All organizations in the retail sector have cyber exposures, which, when they come to light, diminish the trust in the consumer economy. Recent breaches have placed a government spotlight on the retail sector with many recent hearings taking place in Congress, specifically to investigate weaknesses in the cybersecurity of the sector. We anticipate that this scrutiny will continue and government will find it has a vested interest in working with security groups to keep retail companies, and their customers, safe from cyber crime.

Willis is encouraged by the U.S. government's broad and diversified approach to managing cyber risk, which includes the SEC's requirement for businesses to assess and report their company's cyber exposures and remediation steps. Building such awareness for businesses and consumers will promote implementation of more steps to protect, mitigate and minimize cyber events and resultant losses.

1 The disclosure was in response to guidance from the U.S. Securities and Exchange Commission, as found in CF Disclosure Guidance, Topic No. 2: Cybersecurity, October 13, 2011, **http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm**

2 **http://www.verizonenterprise.com/resources/reports/es_data-breach-investigations-report-2013_en_xg.pdf**

3 **http://money.cnn.com/2014/02/04/technology/security/target-senate/**

4 **http://www.emvco.com/**

5 **http://securitywatch.pcmag.com/internet-crime/320071-smart-chip-credit-cards-wouldn-t-have-saved-target**

6 A.B 370.

7 For example see **http://jenner.com/system/assets/publications/12548/original/FTC_Signals_2014_Enforcement_Priorities___Dec_2013.pdf?1386801658#page=1**

8 But note that the number of firms in this group was very small and this may have influenced the outcome.

9 **http://www.nist.gov/cyberframework/index.cfm**

Willis North America Inc.

Brookfield Place
200 Liberty Street, 7th Floor
New York
New York 10281-1003
United States
Tel: +1 212 915 8888

www.willis.com